

PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 4.6.2003

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T



Hakija
Applicant

Nokia Corporation
Helsinki

Patentihakemus nro
Patent application no

20025036

Tekemispäivä
Filing date

02.08.2002

Kansainvälinen luokka
International class

H04Q

Keksinnön nimitys
Title of invention

"Menetelmä SIM-toiminteen järjestämiseksi digitaaliseen langattomaan päätelaitteeseen sekä vastaava päätelaitte ja palvelin"

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä Patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kalla
Tutkimussihteeri

Maksu 50 €
Fee 50 EUR

Maksu perustuu kauppa- ja teollisuusministeriön antamaan asetukseen 1027/2001 Patentti- ja rekisterihallituksen maksullisista suoritteista muutoksineen.

The fee is based on the Decree with amendments of the Ministry of Trade and Industry No. 1027/2001 concerning the chargeable services of the National Board of Patents and Registration of Finland.

Osoite: Arkadiankatu 6 A Puhelin: 09 6939 500 Telefax: 09 6939 5328
P.O.Box 1160 Telephone: + 358 9 6939 500 Telefax: + 358 9 6939 5328
FIN-00101 Helsinki, FINLAND

MENETELMÄ SIM-TOIMINTEEN JÄRJESTÄMISEKSI DIGITAALISEEN LANGATTO- MAAN PÄÄTELAITTEESEEN SEKÄ VASTAAVA PÄÄTELAITTE JA PALVELIN

Keksinnön kohteena on menetelmä SIM-toiminteen (Subscriber Identity Module) järjestämiseksi tiedonsiirtoverkossa viestivään digitaaliseen langattomaan päätelaitteeseen, jossa sanotun SIM-toiminteen yhteyteen kuuluu suoritintoiminnallisuus ja muistivälineet sovellus-, tilaaja- ja verkospesifisen datan tallentamiseksi ja jossa päätelaitteen yhteyteen kuuluu lisäksi suoritintoiminnallisuus dynaamisten sovellusten suorittamiseksi. Keksintö koskee myös vastaavaa päätelaitetta ja palvelinta.

Matkaviestinjärjestelmissä käytetään nykyisin yleisesti erityisesti älykorttisovelluksia. Näitä käytetään erottamaan matkaviestintipäätelaite ME (Mobile Equipment) niin sanottuun yleiseen, määritellyn tyyppisessä matkaviestinverkossa toimivaan laitteisto-osaan sekä erilliseen verkko-/tilaajaspesifiseen osaan, joka yleisemmin tunnetaan myös tilaajaidentiteettimoduulin eli niin sanottuna SIM-toiminteenä (Subscriber Identity Module).

Päätelaitteilla viestiminen asetetussa tiedonsiirtoverkossa vautii nykyisin pääsääntöisesti tilaajaliittymän. Liittymällä identifioidaan muun muassa yksi tai useampia tiedonsiirtoverkkoja, joissa viestintä on sallittua ja tilaajaliittymän liittyviä yksityiskohtaisia asetuksia, joihin kuuluu esimerkiksi verkko-/operaattorikohtainen data (mm. salausalgoritmit) ja tilaajakohdainen data, kuten esimerkiksi matkaviestintilaajatunnus IMSI (International Mobile Subscriber Identity).

30

Data tallennetaan tunnetun tekniikan mukaisesti pienelle, päätelaitteeseen liitettylle ja fyysisesti toteutetulle piilastulle. Lastulle on järjestetty ainakin tallennusvälineet edellä mainittun datan tallentamiseksi ja käyttämiseksi päätelaitteessa sekä mahdollinen suoritinyksikkönä toimiva mikrokontrolleri. Suoritintoiminnallisuus voi joissain ympäristöissä olla myös järjestettyä itse varsinaiseen päätelaitemoduuliin. Pääsääntöisesti

SIM-toiminne on yleensä kuitenkin järjestetty muoviselle alustalle kompaktiksi ja fyysiseksi kokonaisuudeksi, jota myös SIM-kortiksi saatetaan kutsua.

5 Tunnetunlaisille SIM-korteille on matkaviestinpäätelaitteessa standardiliitintä, jossa on kytkentänastat sen sähköiseksi liittämiseksi päätelaitteeseen. SIM-kortin yleisrakenteeseen kuuluu sille järjestetyn mahdollisen mikrokontrollerin lisäksi erilaisia tallennusvälineitä ja apupiirejä, jotka liittyvät esimerkiksi 10 si sen sisäisen tiedonsiirron ja käyttöjännitteiden hallintaan.

SIM-kortille mahdolliesti sijoitetulla mikrokontrollerilla suoritetaan SIM-sovellusta, joilla tunnetusti on useita eri valmistajia. Tunnetussa tekniikassa verkko-operaattorit tai vastaavat 15 tilaajaliittymäpalveluiden tarjoajat antavat näille valmistajille omat ohjeensa ja asetuksensa, joiden mukaisia SIM-sovellukset sitten loppujen lopuksi ovat. Sovellukseen on sisällytetty muun muassa mikrokontrollerin käskykanta ja tiedostoviittaukset tallennusvälineisiin järjestetyn verkko-, päätelaitte- ja tilaajataan 20 lukemiseksi, tulkitsemiseksi ja päivittämiseksi sekä autentikointi- ja salausalgoritmien suoritus.

Matkaviestinalalla on jo pidemmän aikaa etsitty ratkaisuja kiinteän SIM-toiminteen korvaamiseksi esimerkiksi juuri M2M-laitteissa. Tunnetun tekniikan mukaiset SIM-toimikortit aiheuttavat 25 ongelmia ja rasitteita lähes poikkeuksetta kaikille päätelaitteiden kanssa toimiville osapuolille. Ensinnäkin päätelaittevalmistajat ja laitejakelijat kokevat ongelmallisena SIM-korttien toimittamisen edellyttämän jakelulogistiikan ja yleensäkin niihin 30 den järjestämisen päätelaitteisiin.

Erään toisen epäkohdan päätelaittevalmistajille muodostaa SIM-korteista aiheutuvat merkittävät kustannuserät sekä niiden päätelaitteille ja laitteistomoduuleille asettamat muotoilu- ja 35 rakennerajoitteet ja yleensäkin kokorajoitukset. Jo pelkästään tunnetun tekniikan mukaisen SIM-kortin vaativien standardiliit-

täntöjen järjestäminen päätelaitteeseen näyttelee merkittävää kustannuserää päätelaitteiden sarjatuotannossa.

Vielä erääksi erityisesti päätelaitetta käyttävään tilaajaan 5 kohdistuvaksi epäkohdaksi voidaan lukea myös tunnetunlaisille SIM-korteille tallennetun datan turmeltumisriski esimerkiksi tilanteessa, jossa virransyöttö päätelaitteeseen syystä tai toisesta katkeaa kesken sillä suoritettavan viestinnän.

10 Tunnettua SIM-toiminteesseen liittyvää tekniikkaa on kuvattu julkaisuissa FI-104139B (Nokia Networks Oy), FI-104937 (Sonera Oyj), WO-98/53629 (Motorola, Inc), EP-1037159A2 (Nokia Mobile Phones LTD.). Näistä julkaisussa FI-104937 (Sonera Oyj) esitetään menetelmä älykorttitoimintein suorittamiseksi, jolla mahdollistetaan palvelukokonaisuuksien toteuttaminen tietoliikenelaitteella. Tämä ei kuitenkaan tarjoa ratkaisua edellä mainituihin epäkohtiin.

Edelleen tunnettua on esimerkiksi tilaajaliittymän vaihtamisen 20 yhteydessä suoritettavat toimenpiteet tilaajakohtaisen datan, kuten esimerkiksi SMS-viestien (Short Data Message) ja puhelinmuistiotietojen siirtämiseksi vanhalta SIM-kortilta uudelle. Toimenpide voidaan suorittaa joko päätelaitteella tai esimerkiksi verkko-operaattorin palvelupisteessä erityisellä konfigurointisovelluksella.

Tämän keksinnön tarkoituksena on saada aikaan uudenlainen menetelmä SIM-toiminteen järjestämiseksi digitaaliseen langattomaan päätelaitteeseen sekä vastaava päätelaitte ja palvelin. Keksinnön 30 mukaisen menetelmän tunnusomaiset piirteet on esitetty patenttivaatimuksessa 1 ja päätelaitteen patenttivaatimuksessa 16 ja palvelimen patenttivaatimuksessa 17.

Erään ensimmäisen sovellusmuodon mukaan päätelaitteeseen voi 35 olla järjestettyynä fyysinen SIM-kortti, jolle on järjestetty pelkkä suoritintoiminnallisuus. SIM-kortti voi olla kuitenkin

järjestettynä siten, että päätelaitetta aktivoitaessa tilaaja-käyttöön ja sen aikana SIM-kortti ei edellytä nykyisen kaltaisia käsittelytoimia.

5 Erään toisen sovellusmuodon mukaan päätelaitteessa ei ole lainkaan fyysisä SIM-korttia. Tällöin päätelaitteen yhteydestä katoaa myös tarve tunnetunlaisille SIM-liitännöille. Tällä saavutetaan lukuisia etuja useiden osapuolien näkökulmasta. Itse päätelaitteen ja sen yhteyteen kuuluvan piirimoduulin koko pienenee 10 merkittävästi, josta on seurauksena esimerkiksi päätelaitteen valmistuskustannuksien pienenneminen.

Edelleen SIM-korttamuus luo merkittävää kustannussäästöä myös esimerkiksi verkko-operaattorille, koska siltä poistuu SIM-korttien toimitustarve. Laitejakelijan ja päätelaitteen loppukäyttäjän näkökulmasta keksinnön mukainen päätelaitte on huomattavasti käyttäjäystäväällisempi johtuen tunnetunlaisen fyysisen SIM-kortin asennustarpeen poistuessa kokonaan. Kaikki osapuollet saavuttavat etua myös siitä, että SIM-datan turmeltumisesta aiheutuvat 20 ongelmat katoavat keksinnön mukaisen menetelmän myötä.

Eräitä, mutta ei kuitenkaan mitenkään rajoittavia esimerkkejä keksinnön mukaisen menetelmän sovelluskohteena olevista langattomista päätelaitteista ovat CDMA- (Code Division Multiple Access), TDMA- (Time Division Multiple Access) ja FDMA- (Frequency Division Multiple Access) teknologioihin perustuvat ratkaisut ja näiden alimäärittelyt mukaan lukien kolmannen sukupolven järjestelmät. Keksintöä voidaan lisäksi soveltaa myös esimerkiksi multimediapäätelaitteissa, joista eräinä esimerkkeinä voidaan mainita digi-tv- ja satelliittivastaanottimet.

Muut keksinnön mukaiselle menetelmälle, päätelaitteelle ja palvelimelle ominaiset piirteet käyvät ilmi oheisista patenttivaatimuksista ja lisää saavutettavia etuja on lueteltu selitysosas 35 sa.

Keksinnön mukaista menetelmää, päätelaitetta ja palvelinta, jota ei ole rajoitettu seuraavassa esitettäviin suoritusmuotoihin, selostetaan tarkemmin viittaamalla oheisiin kuviin, joissa

- 5 Kuva 1 esittää kaaviokuvana esimerkkiä eksinnön mukaisen menetelmän eräästä sovellusympäristöstä,
- Kuva 2 esittää esimerkkiä eksinnön mukaisesta menetelmästä SIM-toiminnettoman päätelaitteen liittyessä ensimmäis- tä kertaa tiedonsiirtoverkkoon vuokaaviona ja
- 10 Kuva 3 esittää esimerkkiä eksinnön mukaisesta menetelmästä SIM-toiminnetta siirrettäessä ensimmäiseltä päätelait- teelta toiselle päätelaitteelle vuokaaviona.

Kuvassa 1 on esitetty kaaviokuvana esimerkki eksinnön mukaisen menetelmän eräästä sovellusympäristöstä. Tässä digitaaliset pää-
15 telitteet, jotka ovat esimerkiksi matkaviestinpäätelaitteita, kuten GSM-puhelimia A, B tai datapäätelaitteita, kuten esimer-
kiksi PC-tietokoneita C, D viestivät langattomasti tiedonsiirto-
verkossa 10, joka esimerkin mukaisessa tapauksessa on GSM-stan-
20 dardin mukainen.

Päätelaitteen A, C yhteyteen voi erään ensimmäisen sovellusmuo-
don mukaan olla järjestettynä fyysinen alustamaton SIM-kortti
11.1, 11.2. Tällöin PC:ltä C suoritettavaan tiedonsiirtoon käy-
25 tetään esimerkiksi sisäistä modeemia tai vastaavaa (ei esitet-
ty). Tällaiselle SIM-kortille 11.1, 11.2 on ominaista se, että
sille ei alustamattomassaan tilassa ole järjestettynä tiedon-
siirtoverkossa 10 (mahdollisesti hätänumeroa lukuun ottamatta)
viestinnän mahdollistavaa SIM-dataa 13.1, 14.1, 13.2, 14.2. Sa-
30 nottuun SIM-dataan kuuluu sen sisältöä mitenkään kuitenkaan ra-
joittamatta ainakin pääosa verkko-operaattorien tai vastaavien
palveluntarjoajien SIM-sovelluksista 13.1, 13.2 ja näiden mah-
dollisesti tarjoamat erikoispalvelut, jotka hyödyntävät esimer-
kiksi sinänsä tunnettua SAT-toiminnetta (SIM Application Tool-
35 kit). Edelleen sanottu SIM-data voi käsittää tilaaja- ja verk-
kospesifistä dataa 14.1, 14.2, kuten esimerkiksi PIN(1/2)- ja

PUK(1/2)-koodit, salaisen K-avaimen, matkaviestintilaajatunnukseen (IMSI) ja algoritmeja, kuten esimerkiksi verkon autentikointiin liittyviä algoritmeja (A3, A8). Sanottuun SIM-dataan voidaan katsoa myös kuuluvaksi esimerkiksi tiedonsiirtoverkkoon 10 5 liittyvä verkkovierailu-informaatio, fyysisen SIM-päätelaitte - rajapinnan käsitteily ja SIM-toiminteeseen kuuluva turva-data, kuten SIM-sarjanumero.

Alustamattomalle SIM-kortille 11.1, 11.2 on kuitenkin järjestetty 10 ty esimerkiksi virtuaalinen suoritintoiminnallisuus ja sen yhteydessä ajettava latauspalvelusovellus, jolla muun muassa suoritetaan SIM-datan suojaaminen lataamisen päätelaitteen A, C ja SIM-rajapinnan välillä. Eräänä mahdollisena, mutta ei kuitenkaan rajoittavana esimerkkinä sanotusta toiminnallisuudesta voidaan 15 mainita JAVA-virtuaalisuoritin SJE (Security Java Engine).

Suoritintoiminnallisuus SJE on järjestetty toimimaan suojatuissa ympäristössä, jolla huolehditaan siitä, että SIM-data 13.1, 14.1, 13.2, 14.2 ei joudu asiattomien osapuolien käsiin. Luotetavan tietoturvan toteuttamisella onkin keksinnön mukaisessa menetelmässä kaikin puolin merkittävä osa. Päätelaitteeseen A, C järjestettävälle tilaajadatalle 14.1, 14.2, salausavaimille ja esimerkiksi ohjelmallisesti toteutetuille verkon autentikointi ja salausalgoritmeille 13.1, 13.2 on suojetut tallennusvälineet. 25 Salaus voidaan toteuttaa esimerkiksi siten, että päätelaitteessa A, C on salaustoiminnallisuuden sisältävä siru tai vaihtoehtoista käyttäen jotain muistin salausmallia.

Erään toisen suoritusmuodon mukaan päätelaitteesta B, D voi 30 puuttua kokonaan fyysisen SIM-kortti. Tällöin PC-tietokoneeseen D voi olla kytkettynä PCMCIA-korttipuhelin eli GSM-modeemi tai WLAN-kortti (Wireless Local Area Network) (eivät esitetty).

Päätelaitteen B, D yhteyteen on järjestetty tällöin virtuaalinen 35 suoritintoiminnallisuus, josta eräänä, mutta ei kuitenkaan rajoittavana esimerkkinä voidaan mainita virtuaalinen, suoja

JAVA-suoritintoiminnallisuus SJE. Sinänsä sanottu JAVA-suoritin SJE voi olla vastaanlainen, jota käytetään nykyisissä kehitetyneimmässä päätelaitteissa.

5 Keksinnön mukaisessa menetelmässä ainakin pääosa SIM-toiminteen toteuttavasta sovellus-, tilaaja- ja verkkospesifisestä datasta, josta mainittiin esimerkkejä (joilla ei kuitenkaan rajata mitenkään ladattavan datan sisältöä) jo ensimmäisen sovellusmuodon tapauksessa, ladataan päätelaitteelle A - D tiedonsiirtoverkon 10 10 kautta. Tästä käytetään jatkossa yhteisnimitystä SIM-data. Fyysisen SIM-kortin puuttuessa ladattavan SIM-datan ei välttämättä tarvitse käsittää fyysisen SIM-päätelaitte -rajapinnan käsitellyn vaadittavaa dataa.

15 Tätä varten päätelaitteiden A - D yhteyteen on järjestetty sano- tun suoritintoiminnallisuuden SJE lisäksi erityinen SIM-lataus- sovellus 16.1 - 16.4 sanotun SIM-datan lataamiseksi tiedonsiirtoverkon 10 tai vastaan kautta päätelaitteelle A - D ja esimerkiksi siirtämiseksi ensimmäiseltä päätelaitteelta A toiselle 20 päätelaitteelle B. Lataussovellukseen 16.1 - 16.4 kuuluu moduuli, joka reitittää SIM-dataa tiedonsiirtoverkosta 10 päätelaitteelle A - D.

Tiedonsiirtoverkon 10 yhteyteen kuuluu eksinnön mukaisen mene- 25 telmän toteuttamiseksi toiminnallisuus 15 sanotun SIM-datan hal- litsemiseksi ja tallennusvälineet 13, 14 SIM-datan säilyttämi- seksi. Sanottu toiminnallisuus 15 sisältää vastaanlaisen rei- titysmoduulin, joka hallitsee SIM-datan latausta päätelaitteille A - D sekä toiminnallisuuden esimerkiksi tilaajadatan synkronoi- 30 miseksi. Hallintatoiminnallisuus 15 on yhteydessä tiedonsiirtoverkon 10 verkkopalvelukerrokseen, jonka kautta palvelu voidaan hoitaa.

Hallinta voidaan käsittää tässä yhteydessä erittäin laajasti. 35 Siihen kuuluu esimerkiksi sanotun reitityksen lisäksi lataus- pyyntöjä tekevien päätelaitteiden A - D autentikointi, latausten

valvonta, SIM-datan siirtoon päätelaitteelta toiselle liittyvien toimintojen hallinta.

Sanottu hallintatoiminnallisuus 15 voidaan järjestää tiedonsiirtoverkkoon 10 usealla tavalla. Erään edullisen suoritusmuodon mukaan sitä ajava palvelin voi sijaita tiedonsiirtoverkon 10 keskuksen 12 yhteydessä, johon on sijoitettu myös esimerkiksi kyseisessä verkossa 10 viestimään oikeutettujen päätelaitteiden A - D kotipaikkarekisteri HLR (Home Location Register) ja viresaipaikkarekisteri VLR (Visitor Location Register).

Näiden rekistereiden lisäksi on kesukseen järjestetty erityinen SIM-toiminnettomenien paikkarekisteri SLR (SIMless Location Register). Sanottu latauspalvelusovellus 15 operoi sanotussa rekisterissä SLR. Rekisteriin SLR kuuluu tallennusvälineet tilaajien ja verkon SIM-datalle 14 sekä SIM-sovelluksille 13. Tilaajien SIM-data voidaan mieltää käsittämään esimerkiksi puhelinmuistodataa ja näiden tallentamia SMS-viestejä. Verkkokohtainen SIM-data sisältää esimerkiksi kyseiselle tiedonsiirtoverkkotyypille ja verkkooptioille ominaista dataa, joka on alan ammattimiehelle ilmeistä. On huomattava, että SIM-toiminnettomenien päätelaitteiden paikkarekisteri SLR voi olla todellisuudessa olla integroituna joko esimerkiksi kotipaikkarekisterin HLR tai viresaipaikkarekisterin VLR yhteyteen.

25

Keksinnön mukaisen menetelmän toiminnallisuus voi erään suoritusmuodon mukaan perustua tiedonsiirtoverkossa 10 suoritettavassa viestinnässä käytettävään signaaliointiin, johon kuuluu yhtenä toiminteena esimerkiksi päätelaitteen A - D sijainninpäivitys 30 (location update). Tilaajan ollessa rekisteröityneenä sanottuun SLR-rekisteriin, tarjotaan hänen tälle lisävuo SIM-latauspalvelun 15 saamiseksi. Myös SIM-toiminnettomenien paikkarekisteriin SLR siirtymiseksi tilaajalla on oltava päätelaitteessaan A - D sen aikaan saavat toiminnot.

35

Kuvassa 2 on esitetty eräs mahdollinen sovellusesimerkki tilanteesta, jossa ilman SIM-toiminnetta varustettu päätelaite B liittyy tiedonsiirtoverkkoon 10 ensimmäisen kerran esimerkiksi silloin, kun käyttäjä on hankkinut uuden tilaajaliittymän. Käyt-
5 täjän kytkettyä päätelaitteeseen B virran, tähän järjestetty käynnistystoiminnallisuus havaitsee päätelaitteesta B puuttuvan SIM-toiminteen (201). Päätelitteessa B aktivoidaan tämän jälkeen SIM-lataussovellus 16.3, jota esimerkiksi suojuatuissa JAVA-ympäristössä SJE aletaan ajamaan.

10

Lataussovellus 16.3 kysyy käyttäjältä mahdollista käyttäjätunnistetta, salasanaa tai muuta vastaavaa tilaajaliittymän yksikä-
sitteisesti identifioivaa tunnistetta tai sen muodostamisessa käytettävää osaa (202). Käyttäjä antaa esimerkiksi päätelaitteen
15 B näppäimistöltä sanotun tunnisteen, jonka perusteella päätelaitte muodostaa käyttäjän tunnisteinformaation käyttäen käyttäjän antaman tunnisten lisäksi esimerkiksi laiteinformaatiota (203.1).

20 Sanottu tunnisteinformaatio lähetetään tiedonsiirtoverkon 10 kautta hallintatoiminnallisuudelle 15, joka vastaanottaa sen ja toteaa kyseisen tilaajan olevan luvallinen lataamaan päätelaitteelleen B SIM-toiminteen (203.2). Jos tilaajalla ei ole SIM-toiminteen lataamisoikeutta sanotussa verkossa 10, niin pääte-
25 laite B blokataan ja sen SIM-lataussovellus 16.3 tekee vastaanlaisen yrityksen seuraavalle löydetylle verolle 10.

Samalla päätelitteessa B viivästytetään käyttäjärajapintaa näytämällä esimerkiksi "SIM-loading" viesti tai vastaava tie-
30 donanto (204). Päätelaitteen B ja hallintatoiminnallisuuden 15 välille muodostetaan tiedonsiirtoyhteys (205.1, 205.2) ja suoritetaan tiedonsiirto SIM-datan 13.3, 14.3 lataamiseksi päätelaitteelle B (206, 207).

35 Päätelaite vastaanottaa sanotun SIM-datan 13.3, 14.3 ja tallentaa sen muistivälineisiinsä (207). Kun data 13.3, 14.3 koko-

naisuudessaan tai mahdollisesti ainakin oleellinen osa siitä on saatu ladattua päätelaitteelle B, aktivoidaan päätelaitteen B virtuaalisessa suojatussa JAVA-ympäristössä SJE SIM-sovellus (208). Kun päätelaitteen B SIM-lataussovellus 16.3 on varmentanut, että kaikki ladattavaksi tarkoitettu SIM-data 13.3, 14.3 on saatu menestyksellisesti ladattua ja tallennettua päätelaitteelle B, päivitetään päätelaitte B pois SIM-toiminnettomien sijaintirekisteristä SLR (209.1). Hallintatoiminnallisuus 15 suorittaa sanotun päivityksen tietokantaansa SLR (209.2).

10

Seuraavaksi päätelaitteen B käyttörajapinta vapautetaan ja käyttäjän salistaan suorittaa tavanomaiset alan ammattimiehelle siinänsä tunnetunlaiset toimenpiteet, joihin kuuluu esimerkiksi käyttäjän ja päätelaitteen autentikointitoimet sanottuun tiedon-15 siirtoverkkoon 10 (211).

Verkon 10 on annettava proseduurin suoritukselle aikaa eikä se saa hylätä vaikka IMSI tai autentikoinnissa tarvittava SRES (Signed REsponse) viipyisivätkin.

20

Kuvassa 3 on esitetty esimerkki keksinnön mukaisesta menetelmästä SIM-toiminnetta siirrettäessä ensimmäiseltä päätelaitteelta toiselle vuokaaviona. Tällainen tilanne voi käyttäjälle tulla eteen esimerkiksi siinä tapauksessa, kun tämä uusii päätelaitteen ja haluaa käyttää vanhaa tilaajaliittymää myös uudessa päätelitteessaan A.

Päätelaitteen B ollessa päällä käyttäjä suorittaa aluksi toimenpiteitä SIM-toimintein siirtämiseksi (301). Näihin toimenpitei-30 siin kuuluu esimerkiksi tilaajakohtaisen datan päivittämistä, kuten esimerkiksi SMS-viestiarkiston ja puhelinmuistiotietojen "siivousta" tarpeettomasta datasta. Toimenpide pienentää muun muassa siirrettävän datan määrää.

35 Päätelaitteen B sovellusvalikosta aktivoidaan SIM-lataussovellus 16.3 ja sieltä valitaan SIM-datan siirtotoiminne. Samalla voi-

daan asettaa salasana tai vastaava tunniste SIM-datan jälleenlaataamiseksi toiselle päätelaitteelle A (ei esitetty). Päätelaitteesta B viivästetään jälleen käyttörajapintaa näytämällä esimerkiksi sen näytöllä "SIM-loading" -viesti (302). Ensimmäisen 5 päätelaitteen B ja hallintatoiminnallisuuden 15 välille muodostetaan tiedonsiirtoistunto SIM-datan 13.3, 14.3 siirtämiseksi tiedonsiirtoverkon 10 kautta (303.1, 303.2).

Päätelaitteelta B lähetetään sanottu SIM-data 13.3, 14.3 ja sen 10 vastaanottaa hallintatoiminnallisuus 15 tallentaen sen tämän yhteyteen järjestettyihin tallennusvälineisiin 13, 14 (304.1, 304.2). Siirretty tuorein tilaajadata synkronoidaan mahdollisen, vanhemman tilaajadatan kanssa (305) ja päätelaitteen B status tiedonsiirron menestyksellisen suorituksen jälkeen päivitetään 15 SIM-toiminnettomien sijaintirekisteriin SLR (306).

Kun päätelaitteen B SIM-lataussovellus 16.3 on myös saanut varmistuksen SIM-datan 13.3, 14.3 siirron onnistumisesta hallintatoiminnallisuuden 15 alaisiin tietokantoihin 13, 14, päätelaitteelta B tuhotaan sanottu SIM-data 13.3, 14.3, jotta se ei pääse osattomien tahojen, kuten esimerkiksi ensimmäisen päätelaitteen B mahdollisen uuden omistajan käsiin (307).

Seuraavaksi käyttäjä voi suorittaa toimenpiteet SIM-toiminteen 25 lataamiseksi toiselle päätelaitteelle A esimerkiksi kuvassa 2 esitettyä proseduuria soveltaen.

Keksinnön mukaisessa menetelmässä sanottu SIM-sovellus- ja tilaajadata 13, 14 on edullisimmin salattua. Eräs tapa salauksen 30 toteuttamiseksi on käyttää salaiseen ja julkiseen salausavaimen perustuvia ratkaisuja, joihin voidaan sovittaa myös useita autentikointi- ja allekirjoitusmenetelmiä. Datalle 13, 14 suoritettavat salauksenpurkuoperaatiot tai SIM-algoritmit suoritetaan myös edullisimmin salattuina. Tämä voidaan suorittaa sulaute-35 tuissa laitteissa laitteistotasolla tai jossain eristetyssä ohjelmistokokonaisuudessa (JAVA KVM). SIM-toiminteen suorittami-

seksi käyttäen tunnettuja API-ohjelmistorajapintoja (Application Protocol Interface), voidaan erään sovellusmuodon mukaan hyödyntää 3GPP/ETSI -työryhmien luonnostelemaa MExE-protokollaa (Mobile Station Application Execution Environment). Siinä tunnistetaessa SIM-toiminnetta lataava tilaaja aukaistaan SIM-sovellukseen käyttämät API:t käyttöön. PC-ympäristössä eristys voidaan suorittaa saman periaatteeen mukaisesti.

Datavirran käsittely suojudun tallennuksen, ilma-rajapinnan ja suojudun prosessointiympäristön välillä on myös edullisimmin salattua tarpeeksi vahvoilla salausmenetelmissä.

Seuraavaksi esitetään muutamia mahdollisia, mutta ei kuitenkaan mitenkään rajoittavia, vaihtoehtoja tietoturvan ja tilaajan autentikoinnin järjestämiseksi esimerkiksi SIM-dataa ladattaessa päätelaitteelle B ja siirrettäessä ensimmäiseltä B päätelaitteelta toiselle päätelaitteelle A.

Ensimmäisessä toteutusvaihtoehdossa kiinnitetään päätelaitteen B kansainvälinen laitetunnus IMEI (International Mobile Equipment Identification) tilaajaan. Tällainen sovellusmuoto on mahdollinen esimerkiksi silloin, kun käyttäjän hankkima päätelaitte B on verkko-operaattorin sponsoroima.

Päätelaitteen B käynnistyttyä lähetetään se tiedonsiirtoverkkoon CM-SERVICE REQ-viestin, jonka yhtenä parametrina voi olla päätelaitteen IMEI-tunnus. Viestillä pyydetään control manager palvelua ja se on sinänsä tunnettu GSM-teknikan standardiviesti. Tiedonsiirtoverkkoon järjestetysti hallintatoiminnallisuus käynnistää IMEI-tunnuksen perusteella SIM-datan latausproseduurin. Hallintatoiminnallisuus käyttää esimerkiksi asymmetristä salausta (RSA) ja salaa päätelaitteen B julkisella salausavaimella lähetettävän SIM-datan. Päätelaitteella B vastaanotettu SIM-data puretaan sen omalla salaisella avaimella ja se tallennetaan suojattuihin tallennusvälineisiin. Salauksen

lisäksi samoilla avaimilla hoidetaan myös SIM-datan allekirjoitus.

Päätelaitteen B julkisen avaimen jakaminen voidaan erään toimintamallin mukaan järjestää siten, että päätelaitteessa B on kiintäästi salainen avain, jolloin verkko 10 etsii IMEI-tunnisteen perusteella päätelaitteen B valmistajan antamaa julkista avainta. Sanottu julkinen avain voi olla päätelaittevalmistajan jakama tai sitä voidaan myös pyytää siltä tunnistusproseduurin aikana.

10 Tilaajaliittymän myyynnin yhteydessä käyttäjälle annetusta käytäjätunnuksesta, joka voi olla esimerkiksi kertakäyttöinen tulee esimerkiksi IMEI-tunnisteen ja muun satunnaistuksen kanssa salainen avain. Yleensäkin riittävän turvallisien tunnisteiden muodostamiseksi voidaan käyttää päätelaitteeseen kiinteästi järjestettyä laiteinformaatiota (piirikomponenttien sisältämää numeroista dataa jne.). Hallintatoiminnallisuuden 15 yhteyteen järjestetyllä vastaavanlaisella laskennalla luodaan julkinen avain.

20 Vastaavasti, kun SIM-toiminne halutaan siirtää ensimmäiseltä päätelaitteelta toiselle, on uuden päätelaitteen IMEI annettava hallintatoiminnallisuudelle 15.

Toisessa vaihtoehdossa tietoturvan ja tilaajan autentikoinnin järjestämiseksi käytetään IMSI-tunnisteen etsintää, jossa IMSI voidaan generoida lennossa. Kun päätelaitte B käynnistetään, se lähetää tiedonsiirtoverkkoon 10 pyynnön sijainninpäivityksen suorittamiseksi tai CM-palvelupyyynnön, joiden parametrina on IMSI. Tiedonsiirtoverkko 10 aktivoi IMSI-tunnisteen perusteella 30 SIM-toiminteen latausproseduurin.

IMSI-tunniste muodostetaan päätelaitteeseen B esimerkiksi siten, että päätelaitteen B käyttäjä syöttää sen tai että se generoidaan tiedonsiirtoverkossa 10. IMSI-tunnistetta käytetään muodostetaan julkinen salausavain päätelaitteelle B tai verolle 10. Toinen tapa on muodostaa operaattorikohtainen IMSI-tunniste,

joka tarkoittaa, että päätelaitteessa B ei ole SIM-toiminnetta. Tällöin hallintatoiminnallisuus 15 kysyy niiden IMSI-tunnisteiden osalta, jotka eivät ole SIM-toiminnettomenien rekisterissä SLR päätelaitteelta B, että annettiinko IMSI-tunniste ulkoapäin. Jos 5 IMSI annettiin ulkoapäin, estetään päätelaitteen B latauspyyntö.

Erään toisen sovellusmuodon mukaan käyttäjän syöttämään tunnukseen lisätään päätelaitteessa informaatiota, kuten esimerkiksi allekirjoitus, jolla jo päätelaite B voi varmentaa käyttäjän 10 validiteetin. Päätelaite B voi myös antaa verkkoon 10 jonkin SIM-toiminteeseen lataukseen dedikoidun IMSI-tunnisteen ja tilaaja tunnistetaan erikseen käyttäjän antamasta tunnuksesta tarkistaen esimerkiksi sen voimassa olon.

15 Itse SIM-datan lataus ja salaus suoritetaan vastaavalla tavalla kuin ensimmäisessä vaihtoehdossa eli hallintatoiminnallisuus 15 kysyy päätelaitteelta B IMEI-tunnisteen tai käytäen käyttäjän tunnuskoodeja.

20 Erään sovellusmuodon mukaan ladattava SIM-sovellusdata 13.1 - 13.4, voi käsittää esimerkiksi vain SIM-logiikkaosioita. Tähän kuuluu esimerkiksi päätelaitteen A - D SIM-toiminteelle lähetämiensä viestien käsittely ja hakemistojen ylläpito. Osa algoritmeista, kuten esimerkiksi salausalgoritmit voivat olla toteutettuina turvallisuussyistä päätelaitteelle A - D laitteiston solulla, jolloin ne ovat sovelluksille API-toiminteen (Application Protocol Interface) takana. Toki myös algoritmien lataaminen tiedonsiirtoverkosta 10 on mahdollista, mutta se kasvattaa myös SIM-toiminteeseen kuluvaa aika.

30

SIM-data 13.1 - 13.4, 14.1 - 14.4 voi olla myös valitulla tavalla tiivistettyä, jolla pienennetään lataamiseen kuluvaa aikaa.

Päätelaitteen A - D SIM-lataussovelluksessa 16.1 - 16.4 ja tiedonsiirtoverkkoon 10 järjestettyyn hallintatoiminnallisuuden 35 SIM-latauspalvelusovelluksessa 15 on edullisemmin toiminnalli-

suus mahdollisten virhetilanteiden käsittelyiseksi. Tällaisia virhetilanteita saattaa syntyä esimerkiksi silloin, jos pääte-laitteesta A - D loppuu kesken SIM-datan 13.1 - 13.4, 14.1 - 14.4 latauksen tai siirron virta. Toinen esimerkki mahdollisten 5 virhetilanteiden aiheuttajaksi on verkkovirheet.

On huomattava, että keksinnön mukaista menetelmää voidaan edullisesti hyödyntää myös muiden äly- ja toimikorttien tapauksessa, joko mahdollaistaen niiden dynaamisen lataamisen tai niiden hyö-10 dyntämisen käyttäjän tunnistetta muodostettessa SIM-toiminnal-lisuutta ladattaessa. Eräitä, mutta ei kuitenkaan rajoittavia esimerkkejä näistä ovat USIM-toiminnallisuus (User Services Identity Module), HST-kortti (Henkilön Sähköinen Tunnistaminen), WIM-kortti (Wireless Identity Module), jota sovelletaan esimer-15 kaksi mobiilissa kaupankäynnissä asiakkaan tunnistamiseen, VISA-kortti ja muut vastaavat maksukorttitoiminteet sekä multi-mediapäätelaitteet, kuten esimerkiksi satelliitti- ja digi-tv-vastaanottimien tilaajamoduulit. Tällöin kuitenkin rekiste-ri/tietokanta -sovelluspalvelu saattaa sijaita tiedonsiirtover-20 kon 10 ulkopuolella. Eräs tapa suojudun tiedonsiirtoistunnon järjestämiseksi on käyttää esimerkiksi verkkoyhdyksytävää.

Tilaajakohtaisen datan roaming-toiminto on myös mahdollinen, kun käyttäjä esimerkiksi vaihtaa verkko-operaattoria. Nämä mahdol-25 listetaan esimerkiksi SMS-viestiarkiston ja puhelinmuiston siirto uuden SIM-toiminteen yhteyteen.

Keksinnön mukaisessa menetelmässä SIM-datan lataaminen tiedon-siirtoverkon 10 kautta on ymmärrettävä hyvin laajasti. Sen li-30 säksi, että SIM-data 13.1 - 13.4, 14.1 - 14.4 ladataan suoraan tiedonsiirtoverkosta 10 päätelaitteelle A - D, voidaan data toimittaa päätelaitteelle A - D myös paikallista tiedonsiirtoverk-koa käyttäen esimerkiksi siten, että se ladataan operaattorin palvelupisteessä PC-tietokoneelta tunnetunlaisella ohjelmointi-35 laitteella sinänsä tunnettuja datalinkki yhteyksiä käyttäen (da-tasuite, serialport, BlueTooth, IrDA) ilman varsinaisen tiedon-

siirtoverkon 10 suoranaista vaikutusta (ei esitetty). Eräänä toisena paikallisena lataustapana voidaan hyödyntää suoraan kahden päätelaitteen B, A välille muodostettavaa yhteyttä (ei esitetty).

5

Edelleen erään suoritusmuodon mukaan päätelaitteeseen A, C voidaan kytkeä niin sanottu SIM-asennusmoduuli. Tämä voidaan järjestää esimerkiksi fyysisen SIM-liitynnän yhteyteen tai muuten paikallisesti (esimerkiksi BT-yhteydellä). SIM-asennusmoduulilla 10 päätelaite A, C pääsee normaalisti tiedonsiirtoverkkoon 10, joka jälkeen joko automaattisesti tai päätelaitteen A, C käyttäjän toimesta voidaan käynnistää proseduuri SIM-toiminteen toteuttamiseksi vaaditun datan lataamiseksi päätelaitteelle A, C.

15 Seuraavassa erätä, mutta ei kuitenkaan mitenkään rajoittavia esimerkkejä tällaista SIM-asennusmoduulia hyödyntävistä tapauksista. Operaattorin myyntipisteessä voidaan kytkeytyä jollain operaattorin erikoistilaajalle (kuten operaattorin sponsoroiman päätelaitteen tapauksessa) tarkoitettulla SIM-asennusmoduulilla 20 verkkoon, jolla sitten tilaajan oma SIM-toiminne ladataan verkosta päätelaitteeseen. Verkko tunnistaa tällöin SIM-toiminteen lataukseen oikeutetun erikoistilaajan. Edelleen myös jollain muulla SIM-kortilla voidaan kytkeytyä verkkoon SIM-toiminteen lataamiseksi SIM-latauspalvelusta päätelaitteelle. Tämän jälkeen 25 SIM-kortti voidaan poistaa päätelaitteesta. SIM-asennuskortilta voidaan myös esimerkiksi siirtää SIM-toiminne päätelaitteelle, jolloin SIM-asennusmoduuli ja päätelaite ovat tiedonsiirtoyhdydessä siirron ajan. Tiedonsiirron jälkeen SIM-asennusmoduuli voidaan poistaa päätelaitteesta.

30

Lisäetuja, joita keksinnön mukaisella menetelmällä saavutetaan, on päätelaitteiden vesitiivis, tukeva ja mekaniikaltaan rei'ätön rakenne ja esimerkiksi suurasiakkaiden, kuten yritysten oleellisesti helpottunut tilaajaliittymien hankinta ja asennus päätelaitteisiin. SIM-korttia ei voi enää anastaa päätelaitteesta 35 eikä erikoistilaajaliittymien SIM-kortteja voida käyttää väärin

(erikoistarifit). Lisäksi SIM-toiminteita voidaan vaihtaa ja koota helposti.

Keksinnön mukainen menetelmällä luodaan tilaajille runsaasti uusia palveluja. Eräänä ensimmäisenä tällaisena hyötyväkökohdana voidaan mainita tilaajaliittymien myynnin ja hankinnan suorittaminen dynaamisesti. Jos päätelaitte A - D on esimerkiksi SIM-toiminnettomassa tilassa, se voidaan asettaa pyytämään tarjouksia tilaajaliittymistä useilta verkko-operaattoreilta. Tällaisissa "huutokauppa" -tilanteissa on päätelaitteessa oltava yleensä jonkinlainen tunniste käyttäjän identifioimiseksi, joka voi esimerkiksi olla WIM-kortti (Wireless Identity Module). Lisäksi päätelaitteelle A - D on tällöin oltava mahdollisuus tarjota tilaajaliittymiä, jopa sellaisessakin tilanteessa, jos päätelitteessa A - D on sellainen jo aktiivisena. Tilaajaliittymän luonne muuttuu dynaamiseksi mikä edellyttää myös dynaamista tilaajadataa operaattoreiden välillä.

Tilaaja saavuttaa eräänä toisena etuna sen, että päätelaitteelle A - D voi keksinnön mukaisen menetelmän myötä ladata useampia tilaajaliittymiä. Tämä on mahdollista, jos päätelaitteen A - D suojaudu suoritinympäristö SJE tukee useampaa kuin yhtä sovellusta. Tällöin eri SIM-toiminteiden välillä suoritettava tilaajadatan synkronisointi voidaan suorittaa tiedonsiirtoverkossa hallintotoiminnallisuuden kautta tai sitten eräänä toisena vaihtoehtona suoraan päätelaitteessa A - D suojuissa suoritusympäristössä SJE SIM-toiminteiden välillä. Kytkentä ensimmäiseltä SIM-toiminteelta toiselle voidaan myös automatisoida.

Eräänä kolmantena etuna saavutetaan tilaajien monistaminen. Kotipaikkarekisterin HLR huipulle voidaan järjestää enemmän toiminnallisuutta käsittelemään samalta tilaajaliittymältä useampia samanaikaisia liittymisiä sanottuun tiedonsiirtoverkkoon. Tällöin tilaajalla voi olla useampia päätelaitteita, joilla on sama tilaajatunniste. Käyttööikeus yhdelle käyttäjän päätelaitteelle voidaan selvitellä päätelaitteen SIM-toiminteeseen ja koti-

paikkarekisterin HLR välillä ilman, että SIM-sovellus jouduttaisiin lataamaan aina jokaiseen käyttäjän päätelaitteeseen.

Keksinnön mukaista menetelmää on edellä selitetty yksittäisen sovellusesimerkin valossa. On itsestään selvää, että proseduraaliset toimintavaiheet keksinnön mukaisen menetelmän toteuttamiseksi voivat sisältää edellä esitetyn lisäksi alivaiheita ja ne voidaan eräissä tapauksissa suorittaa myös edellä poikkeavissa järjestyksissä (esimerkiksi verkko-operaattorista riippuen).

10

On ymmärrettävä, että edellä oleva selitys ja siihen liittyvät kuvat on tarkoitettu ainoastaan havainnollistamaan esillä olevaa keksinnön mukaista menetelmää, päätelaitetta ja palvelinta. Keksintöä ei siten ole rajattu pelkästään edellä esitettyihin tai patenttivaatimuksissa määriteltyihin suoritusmuotoihin, vaan alan ammattimiehelle tulevat olemaan ilmeisiä monet erilaiset keksinnön variaatiot ja muunnokset, jotka ovat mahdollisia oheisten patenttivaatimusten määrittelemän keksinnöllisen ajatuksen puitteissa.

PATENTTIVAATIMUKSET

1. Menetelmä SIM-toiminteen (Subscriber Identity Module) (11.1) järjestämiseksi tiedonsiirtoverkossa (10) viestivään digitaali-
seen langattomaan päätelaitteeseen (A, D), jossa sanotun SIM-
toiminteen (11.1) yhteyteen kuuluu suoritintoiminnallisuus ja
muistivälineet sovellus-, tilaaja- ja verkkospesifisen datan
(13.1, 13.4, 14.1, 14.4) tallentamiseksi ja jossa päätelaitteen
(A, D) yhteyteen kuuluu lisäksi suoritintoiminnallisuus (SJE)
10 dynaamisten sovellusten suorittamiseksi, tunnettu siitä, että
ainakin pääosa SIM-toiminteen toteuttavasta sovellus-, tilaaja-
ja verkkospesifisesta datasta (13.1, 13.4, 14.1, 14.4) ladataan
päätelaitteelle (A, D) tiedonsiirtoverkon (10) kautta.
- 15 2. Patenttivaatimuksen 1 mukainen menetelmä, tunnettu siitä,
että päätelaitte (A, D) ja tiedonsiirtoverkko (10) varustetaan
latausovelluksella (16.1, 16.4, 15) sanotun SIM-datan (13.1,
13.4, 14.1, 14.4) lataamiseksi.
- 20 3. Patenttivaatimuksen 1 tai 2 mukainen menetelmä, tunnettu sii-
tä, että sanotun tiedonsiirtoverkon (10) yhteyteen kuuluu toi-
minnallisuus (15) sanotun SIM-datan hallitsemiseksi ja välineet
(13, 14) sen tallentamiseksi.
- 25 4. Jonkin patenttivaatimuksen 1 - 3 mukainen menetelmä, tunnettu
siitä, että ilman SIM-toiminnetta varustetun päätelaitteen (A,
D) liittyessä tiedonsiirtoverkkoon (10), vaiheittain
30 - muodostetaan päätelaitteella (A, D) tunnisteinfor-
maatio asetetun SIM-datan (13.1, 13.4, 14.1, 14.4)
lataamiseksi (202),
 - lähetetään tunnisteinformaatio tiedonsiirtoverkon
 (10) yhteyteen järjestetylle hallintatoiminnallisuute-
delle (15) (203.1),
 - muodostetaan ja suoritetaan päätelaitteen (A, D) ja
35 hallintatoiminnallisuuden (15) välinen tiedonsiirtois-
tunto sanotun SIM-datan (13.1, 13.4, 14.1, 14.4) la-

taamiseksi päätelaitteelle (A, D) (205.1 - 205.2, 206
- 207),
- suoritetaan päätelaitteella (A, D) SIM-sovellus
(208) ja
5 - vapautetaan päätelaitteen (A, D) käyttäjärajapinta
(210).

5. Jonkin patenttivaatimuksen 1 - 4 mukainen menetelmä, tunnettu
siitä, että siirrettäessä SIM-toiminnetta ensimmäiseltä pääte-
10 laitteelta (A) toiseen päätelaitteeseen (B) vaiheittain

- suoritetaan ensimmäisellä päätelaitteella (A) mah-
dollisia toimenpiteitä SIM-toiminteen siirtämiseksi
(301),
- muodostetaan ja suoritetaan ensimmäisen päätelait-
15 teen (A) ja hallintatoiminnallisuuden (15) välinen
tiedonsiirtoistunto sanotun SIM-datan (13.1, 13.4,
14.1, 14.4) siirtämiseksi hallintatoiminnallisuuden
(15) yhteyteen (303.1, 303.2, 304.1, 304.2),
- synkronoidaan hallintatoiminnallisuuden (15) yh-
20 teeen järjestettyä ja päätelaitteelta (A) siirrettyä
dataa (305) ja
- liitytään sanotulla toisella päätelaitteella (B)
tiedonsiirtoverkkoon (10) tunnistetiedoiltaan saman
SIM-toiminteen lataamiseksi.

25 6. Patenttivaatimuksen 5 mukainen menetelmä, tunnettu siitä,
että muodostetaan lisäksi tunnisteinformaatio uuden SIM-toimin-
teen aktivoimiseksi.

30 7. Patenttivaatimuksen 6 mukainen menetelmä, tunnettu siitä,
että sanotun tunnisteinformaation muodostamiseen käytetään pää-
telaitteen (A) yhteyteen järjestettyä laitteistonpesifistä da-
taa.

8. Patenttivaatimuksen 4 tai 5 mukainen menetelmä, tunnettu siitä, että yhtenä osavaiheena päivitetään päätelaitteiden (A, B) SIM-toiminteen statustila.

5 9. Jonkin patenttivaatimuksen 5 - 8 mukainen menetelmä, tunnettu siitä, että yhtenä osavaiheena hävitetään ensimmäiseltä päätelaitteelta (A) SIM-data.

10. Jonkin patenttivaatimuksen 1 - 9 mukainen menetelmä, tunnettu siitä, että päätelaitteeseen (A, B) on järjestetty fyysinen SIM-toimikortti, johon kuuluu dynaaminen suoritinympäristö (SJE) ladattujen sovellusten suorittamiseksi.

11. Jonkin patenttivaatimuksen 1 - 10 mukainen menetelmä, tunnettu siitä, että ainakin osa ladattavasta ja/tai siirrettävästä datasta (13.1, 14.1) on tiivistettyä.

12. Jonkin patenttivaatimuksen 1 - 11 mukainen menetelmä, tunnettu siitä, että ainakin osa ladattavasta ja/tai siirrettävästä datasta (13.1, 14.1) on salattua.

13. Jonkin patenttivaatimuksen 1 - 12 mukainen menetelmä, tunnettu siitä, että sanottu SIM-sovellusdata (14.1) käsittää SIM-logiikkaa.

25

14. Jonkin patenttivaatimuksen 1 - 13 mukainen menetelmä, tunnettu siitä, että sanottu SIM-sovellusdata (14.1) käsittää algoritmeja, kuten esimerkiksi verkon autentikointiin ja/tai salaukseen liittyviä algoritmeja.

30

15. Jonkin patenttivaatimuksen 1 - 14 mukainen menetelmä, tunnettu siitä, että SIM-datan (13.1, 14.1) lataaminen päätelaitteelle (A, B) suoritetaan paikallisesti.

35 16. Digitaalinen langaton päätelaite (A, D), jonka yhteyteen on järjestetty SIM-toiminne (Subscriber Identity Module) (11.1),

joka käsittää suoritintoiminnallisuuden ja muistivälineet sovellus-, tilaaja- ja verkkospesifisen datan tallentamiseksi (13.1, 14.1, 13.4, 14.4) ja jossa päätelaitteen (A, D) yhteyteen on järjestetty lisäksi suoritintoiminnallisuus (SJE) dynaamisten 5 sovellusten suorittamiseksi, tunnettu siitä, että ainakin pääosa SIM-toiminteen toteuttavasta sovellus-, tilaaja- ja verkkospesifisestä datasta (13.1, 14.1, 13.4, 14.4) on järjestetty ladatavaksi päätelaitteelle (A, D) tiedonsiirtoverkon (10) kautta.

10

17. Palvelin (12) SIM-toiminteen järjestämiseksi digitaaliseen langattomaan päätelaitteeseen (A, D), jossa palvelin (12) on järjestetty tiedonsiirtoverkon (10) yhteyteen ja jossa SIM-toiminteeseen kuuluu sovellus-, tilaaja- ja verkkospesifistä dataa 15 (13.1, 14.1, 13.4, 14.4), tunnettu siitä, että palvelimella (12) on toiminnallisuus (15) sanottuun SIM-toiminteeseen kuuluvan datan hallinnoimiseksi ja välineet (13, 14) säilyttämiseksi ja jossa hallinnoimistoiminnallisuuden (15) yhteyteen on järjestetty reitityssovellus sanotun SIM-datan (13.1, 14.1, 13.4, 14.4) 20 lataamiseksi sanotulle päätelaitteelle (A, D) tiedonsiirtoverkon (10) kautta.

(57) TIIVISTELMÄ

Keksintö koskee menetelmää SIM-toiminteen (Subscriber Identity Module) (11.1) järjestämiseksi tiedonsiirtoverkossa (10) viesti-vään digitaaliseen langattomaan päätelaitteeseen (A, D). Sanotun SIM-toiminteen (11.1) yhteyteen kuuluu suoritintoiminnallisuus ja muistivälineet sovellus-, tilaaja- ja verkkospesifisen datan (13.1, 13.4, 14.1, 14.4) tallentamiseksi. Päätelaitteen (A, D) yhteyteen kuuluu lisäksi suoritintoiminnallisuus (SJE) dynaamisten sovellusten suoritamiseksi. Menetelmässä ainakin pääosa SIM-toiminteen toteuttavasta sovellus-, tilaaja- ja verkkospesifisestä datasta (13.1, 13.4, 14.1, 14.4) ladataan päätelaitteelle (A, D) tiedonsiirtoverkon (10) kautta.

Kuva 1.

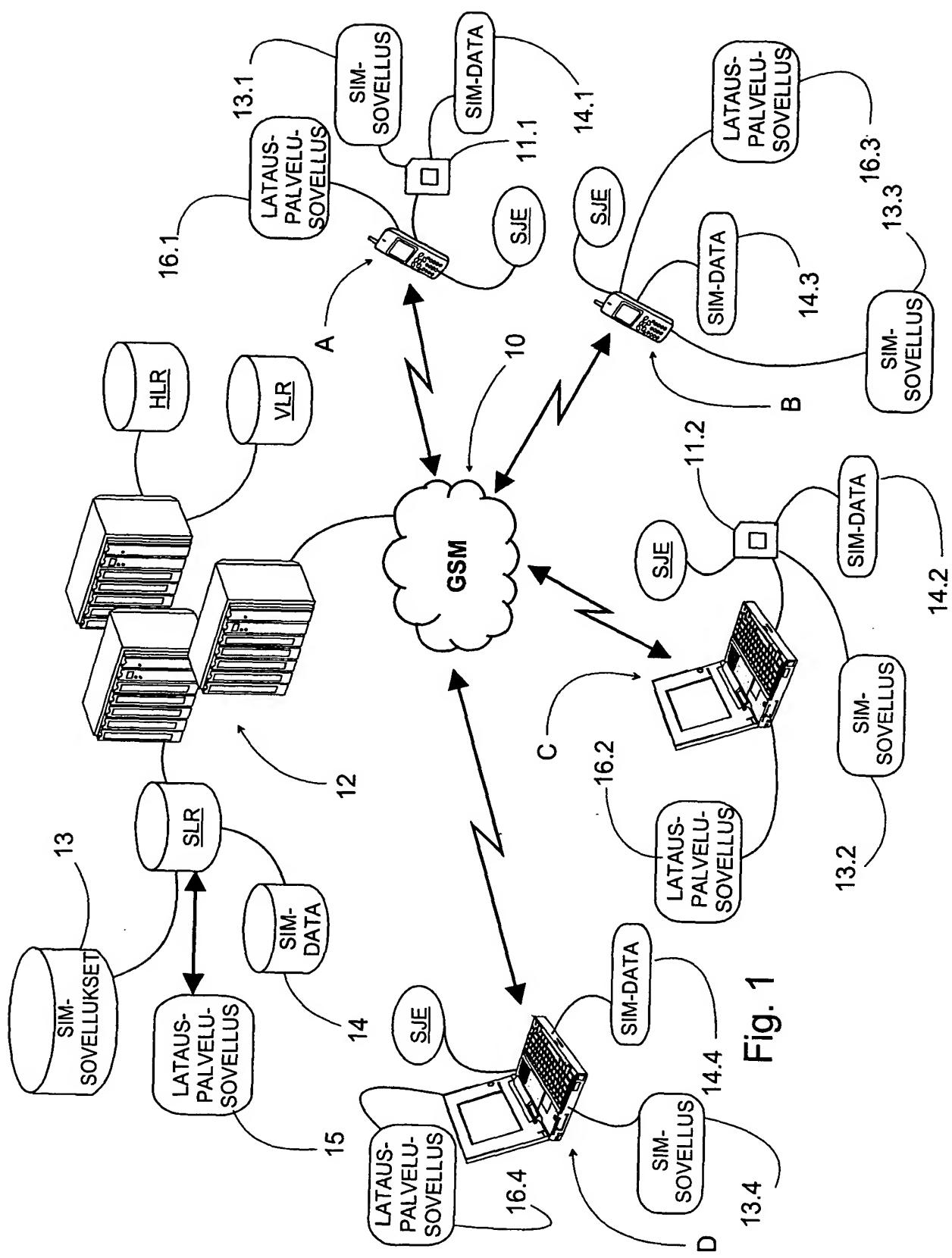


Fig. 1

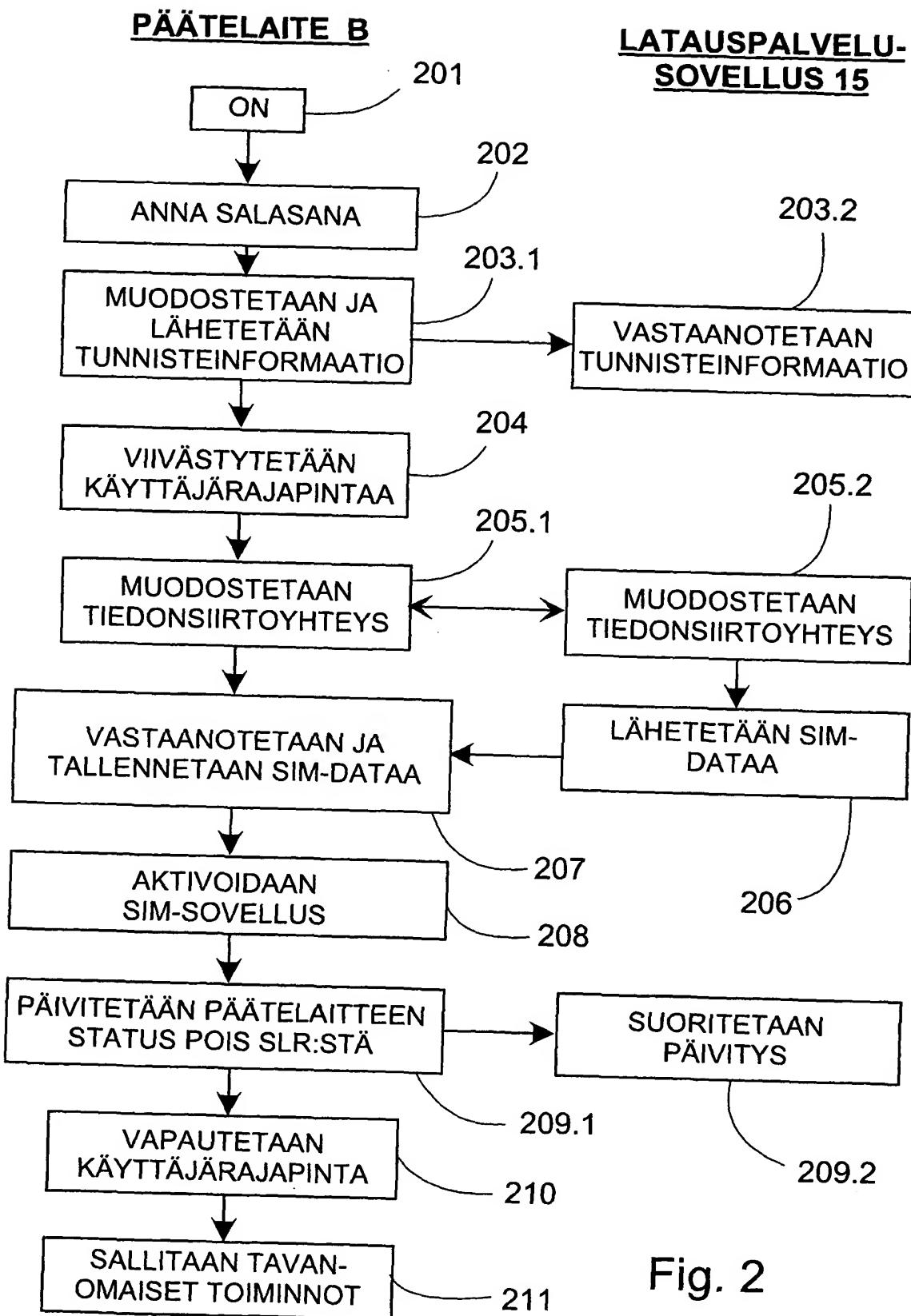


Fig. 2

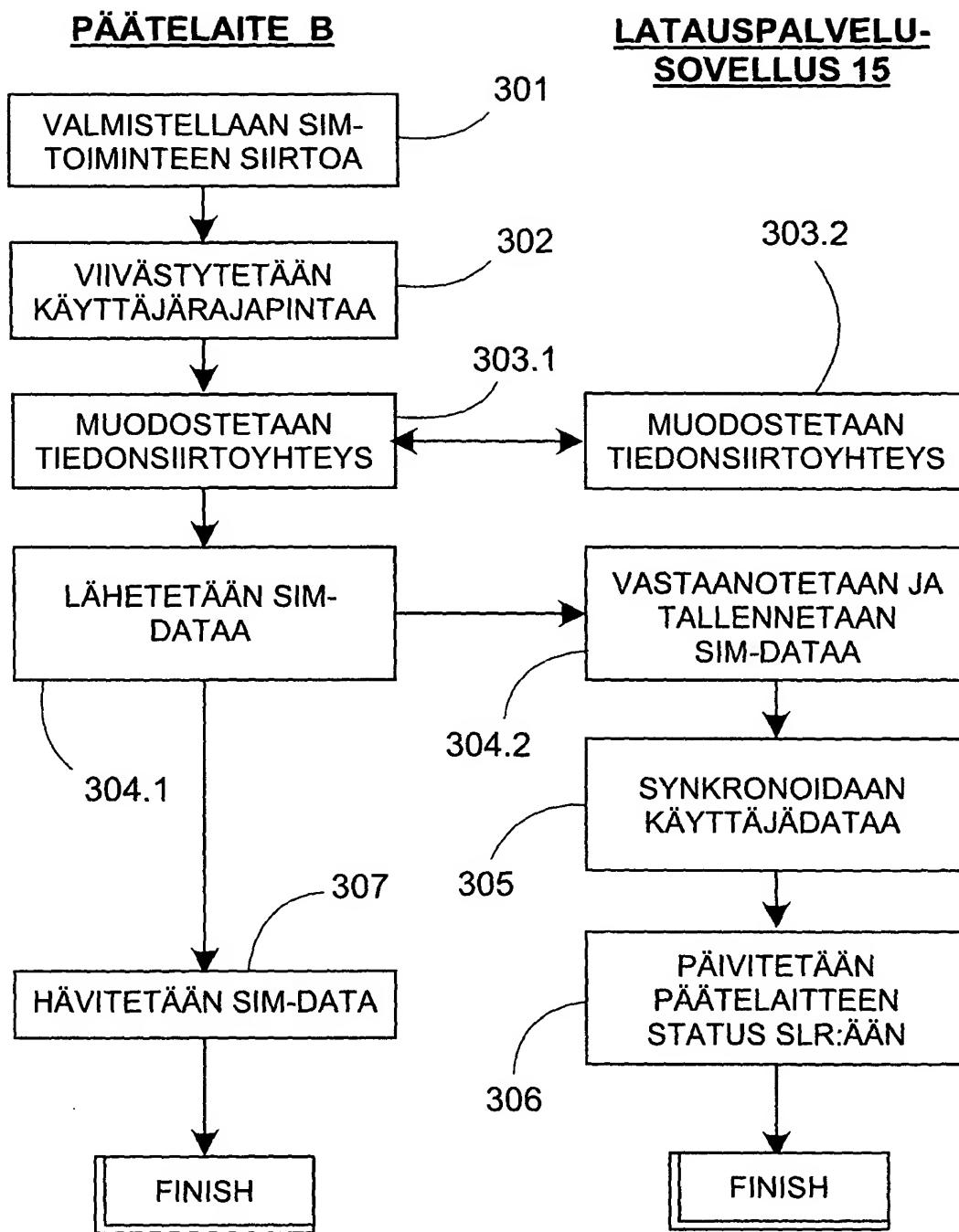


Fig. 3